fraudulent calls that could have been, in any measure, prevented had this information been provided. If called and calling number information is provided, liability analysis should focus on the extent to which the exchange carrier has utilized its detection systems and other available information to prevent the loss from occurring. If the exchange carrier has acted responsibly, the loss should ultimately lie with either the end user customer or the underlying network service provider. If the exchange carrier has not acted responsibly, the relative negligence of all involved parties should determine their share of the loss.

3. Tariff Limitations of Liability v. Allocation of Liability.

The Commission seeks comment on whether existing tariff limitations of liability "should be permitted to shield the LECs from responsibility for toll losses incurred when a joint use calling card is used to bill fraudulent calls or whether the Commission should establish a rule for allocating liability for toll losses." (*NPRM* at ¶ 39.) GTE believes that, if the exchange carrier's LIDB functions properly and incorporates reasonable fraud detection methods, the exchange carrier should not be liable for losses on another company's long distance services; *i.e.*, the underlying IXC.[31] The exchange carrier does not share in the revenues for that long distance service and it should not be assigned a portion of the losses.[32]

GTE agrees with the Commission that "there may be many different fact patterns each time a loss is generated, making the development of a general rule difficult." (*Id.*)

---

[31] As a LIDB owner, GTE *does* assume liability for toll fraud that results from a failure of its LIDB or from erroneous GTE-supplied LIDB data. *See NPRM* at ¶ 38.

[32] The only exception occurs when the calling card is used in the service territory of the issuing exchange carrier. In that case, the exchange carrier receives access charges for the portion of the call that it handled. This generally is a small portion of the total value of the call.

It simply would not be feasible to capture all possible scenarios in a tariff due to the thousands of known ways in which calling card fraud may occur. Moreover, as discussed above, each entity involved in providing calling cards and calling card services already has adequate incentive to prevent calling card fraud. In some cases, existing business arrangements between IXCs, LECs, and LIDB owners already include loss sharing arrangements.

GTE opposes an arbitrary liability allocation scheme. Should the Commission nevertheless develop one, it is imperative that the LECs' good faith efforts be factored in. Liability for losses incurred that are totally beyond the control of the LEC should not be allocated to the LEC. Any liability allocation rules should permit Price Cap exchange carriers to reflect allocated losses through exogenous treatment. Such an administrative mandate clearly would be "beyond the control of the carrier."[33] Exogenous cost recovery would be fully consistent with the recovery mechanism specified by the Commission for the costs associated with implementation and operation of 800 Data Base access service.[34] In that proceeding, the Commission required that the costs of implementing a new method of providing 800 access service be recovered through a per query rate, rather than achieving recovery through generally higher switched access rates to all customers.[35] Incorporating toll fraud liability into LIDB query rates would be consistent with Commission requirements in the 800 Data Base access service proceeding.

---

[33] *Policy and Rules Concerning Rates for Dominant Carriers*, Second Report & Order ("Second Price Cap Order"), CC Docket No. 87-313, 5 FCC Rcd 6786, 6807 (1990).

[34] *See, In the Matter of Provision of Access for 800 Service*, Second Report and Order, 8 FCC Rcd 907, 911 (1993).

[35] *Id.* at 909.

In summary: GTE and other LIDB owners, as well as LIDB customers, are already actively engaged in calling card fraud prevention and detection. No "artificial" incentives are needed for exchange carriers to continue in their fight against toll fraud. "Natural" incentives are already in place. The success of exchange carrier efforts is highly dependent upon cooperation between end user customers and other network service providers. Any exchange carrier that has reasonable fraud prevention measures in place and operating properly should not be arbitrarily allocated a share of interLATA or international toll fraud liability.

E. OTHER PROPOSALS AND REQUESTS FOR COMMENT.

1. Effect of Billing and Collection Agreements on Toll Fraud Prevention Incentives.

The Commission seeks input on the impact of existing billing and collection ("B&C") agreements between IXCs and exchange carriers on their incentives for toll fraud prevention. (*NPRM* at ¶ 41.) B&C agreements between exchange carriers and IXCs already include both direct or indirect incentives for exchange carriers to address toll fraud.[36]

GTE has a number of B&C agreements with IXCs. The assignment of responsibility for revenue losses varies across agreements, but one fact is common to all – GTE bears *all* of the liability for unbillable calls if GTE actions or omissions cause the loss. As an example, if a customer instructs GTE to disconnect a telephone on a certain date and GTE fails to do so, GTE is totally responsible for any toll fraud that may occur after the disconnect due date.

---

[36] Losses from toll fraud may be associated with either unbillable or uncollectible calls. Unbillable calls are those for which no party responsible for payment can be identified. Uncollectible calls are those that are billable, but for any number of reasons, no revenues can be obtained.

B&C agreements with some IXCs include provisions whereby GTE accepts a certain level of liability for uncollectibles.[37] GTE's liability is negotiated by GTE and the IXC and considers a variety of factors: contract minimums; rate levels paid by the IXC for billing activities; and the type of traffic being billed. If uncollectibles are higher than the predetermined amount, then GTE assumes the excess. On the other hand, B&C agreements with other IXCs may not include any GTE responsibility for uncollectibles. Nevertheless, those IXCs certainly expect the exchange carrier to be actively engaged in fraud prevention. If the exchange carrier is not diligent, the IXC always has the option of performing its own billing function, resulting in a loss of business to the LEC. Thus, under either B&C arrangement, financial incentives exist for GTE to actively prevent and detect toll fraud.

2. The Effect of Network Changes on Toll Fraud Prevention and Detection.

The Commission also seeks comment on network changes that could influence toll fraud detection and prevention. (*NPRM* at ¶ 41.) Originating Line Number Screening ("OLNS") is one method of fraud prevention and detection that the industry currently is exploring. This is not a new concept as it was proposed originally to be part of LIDB. OLNS would provide information on the originating line and what types of calls are allowed to be made from that line. It would require an IXC or operator services provider to query a LIDB before processing the call.

Presently, most LECs send special information digits ("II digits") that indicate to the IXC that special handling is required.[38] The LEC provides the IXC, via paper records, a database of lines having these II digits. However, this is a cumbersome and

---

[37] Toll fraud is only one portion of uncollectibles. Other components include customers who cannot pay a bill and customers who move to avoid paying a bill.

[38] For example, the "06" digits are used for hotels and motels, while the "07" digits are used for calls requiring special handling like coinless payphones or hospitals.

time consuming process. Thus, the IXCs want the LECs to provide a service sometimes referred to as "Flexible ANI." With this service, the LEC would forward II digits indicating that the originating line requires special handling (*i.e.*, different II digits for cellular, private payphones, hotels/motels, etc.) to the IXC in the Automatic Number Identification ("ANI") information sequence. Technically this is a very expensive proposition for the LECs as each time a new set of digits is agreed upon by the industry, the software in all LEC switches must be updated.

GTE proposes that with the advent of the Intelligent Network ("IN") it makes sense to distribute this form of information processing to centralized databases, the LIDB being an ideal application. Interconnection would be accomplished via the existing SS7 network. When a call is placed that requires alternate billing (*e.g.*, calling card, bill-to-third, or collect), the operator services provider handling the call would query the LIDB to validate that the originating line is allowed Alternate Billing Service ("ABS") calling features. While this is a viable solution, it is opposed by some IXCs and LECs because of the associated costs. LECs would experience the additional costs associated with updating their LIDBs and the network equipment required to route the additional calls. IXCs are opposed to OLNS on the grounds that it would require them to "double-dip." That is, they would have to query the LIDB twice, once to check to see if the call is allowed to be processed and again to obtain information on the line being billed, thereby increasing the IXC's cost for LIDB validations. Nevertheless, GTE believes that this is a possible solution and that the industry should be allowed to continue to work on it in the existing ATIS Toll Fraud Prevention Committee.[39] This effort is further indication that the industry is capable of addressing fraud detection without Commission intervention.

---

[39] *See* n.2, *supra.*

3. Carrier Release of Network Change Information.

The Commission seeks comment on "how, when, and where a carrier should release [network change] information" that could influence toll fraud detection or prevention. (*NPRM* at ¶ 41.) GTE does not believe that network changes associated with toll fraud detection or prevention should be treated any differently from other network changes. LECs and IXCs should continue the existing practice of informing all interconnecting telecommunications service providers whenever a network change occurs that could impact other providers.

The sharing of network upgrade information already occurs on a regular basis. As a practical business matter, a network provider must ensure that the services it furnishes to customers are not disrupted. This requires coordination with all interconnecting network providers to ensure services continue to function properly. In addition, Commission rules already require notification of network upgrades.

GTE regularly meets with its customers and other network providers to discuss planned new network capabilities. Some network changes are only new ways of provisioning existing services. GTE coordinates implementation of these types of network changes with connecting network providers before the new functionality is deployed. This is necessary to ensure that existing services continue to function properly. Whenever network changes enable the offering of a new service, GTE informs connecting network providers prior to filing tariffs for the new service. The tariff approval process also provides public notice that new network capabilities are available. Industry forums also are very useful in informing all interested parties of new network capabilities. Groups such as the Ordering and Billing Forum ("OBF") routinely address issues associated with orders for service and proper billing. The ATIS Toll Fraud Prevention Committee offers another forum to discuss toll fraud network upgrades.

In addition to the above, GTE and other exchange carriers currently are subject to several existing network information disclosure requirements. The Commission's All Carrier Rule[40] and Part 68.110[41] network information disclosure rules, as well as similar provisions in the GTE Consent Decree,[42] obviate the need for any further Commission action to require dissemination of information regarding implementation or installation of network changes impacting toll fraud.

The All Carrier Rule and Section 68.110 rules are premised upon the need to provide ample notice to LEC customers of changes which may impact either their interface to the network or the operation of their terminal equipment.[43] The All Carrier Rule requires "that all information relating to network design be released to all interested parties on the same terms and conditions, insofar as such information affects either intercarrier interconnection or the manner in which interconnected CPE operates."[44]

Section 68.110 requires all LECs to provide relevant information to all customers regarding network changes that would impact the function of CPE if changes:

> [c]an be reasonably expected to render any customer's terminal equipment incompatible with telephone company communications

---

[40] *Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry)*, Final Decision, 77 F.C.C.2d 384 (1980), *reconsideration*, 84 F.C.C.2d 50, 82-83 (1980) ("*Computer II Reconsideration Order*") (subsequent citations omitted).

[41] 47 CFR Section 68.110.

[42] *U.S. v. GTE Corp.*, Trade Cas. (CCH) ¶66,355 (D.D.C. 1985)(the "GTE Consent Decree").

[43] GTOC Tariff FCC No. 1, Section 2.1.7 incorporates the All Carrier Rule and Section 68.110.

[44] *Computer II Reconsideration Order*, 84 F.C.C.2d at 82-83.

Further, GTE's Consent Decree states:[45]

> No GTOC shall discriminate between the interexchange telecommunications services, information services, or customer premises equipment of GTE (including any information services of a GTOC) and the interexchange telecommunications services, information services, or customer premises equipment of other persons in the:
>
> 1. establishment and dissemination of technical information and interconnection standards;
>
> 2. interconnection and use of the GTOC's exchange telecommunications or exchange access services and facilities or in the charges for each element of service; and
>
> 3. provision of new exchange access and information access services and the planning for and implementation of the construction or modification of facilities used to provide exchange access and information access.

In summary: GTE's billing and collection agreements provide both direct and indirect incentives for toll fraud prevention and detection. One promising network-based prevention tool currently being evaluated by the industry is Originating Line Number Screening. Existing customer-service provider relationships, industry forums, and Commission rules are more than adequate to inform all interested parties of network changes that could influence toll fraud detection or prevention.

IV. THERE ARE ACTIONS THE COMMISSION CAN TAKE TO ASSIST IN COMBATING TOLL FRAUD.

In response to the Commission's query as to "what other actions ... [it] ... should take to further fraud prevention" (*NPRM* at ¶ 41) GTE recommends the following.

A. PAYPHONE ACTIVITIES.

Private payphone providers are unique in that they are often individuals rather than companies. For these parties, GTE suggests that the Commission encourage or require organizations representing the interests of these parties make available to their

---

[45] *See* GTE Consent Decree, Section V.B.

members, on a current and regular basis, information on fraud prevention. Newcomers to the private payphone business should be made to bear the responsibility for seeking information on fraud either through one of these organizations or from the LEC. Ongoing prudent business practices bearing on fraud prevention should not be ignored simply because a subscriber has purchased one tool (*e.g.*, LEC blocking or screening services) to aid in fraud prevention.

B. CUSTOMER INFORMATION ACTIVITIES.

Another area in which the Commission can assist in limiting toll fraud involves establishing an environment whereby exchange carriers, IXCs, and operator services providers are allowed to share customer information that is used in fraud prevention or detection. Today many criminals simply move to another exchange carrier territory or to another IXC's network to avoid capture. The Commission could assist the industry in limiting toll fraud by spearheading an effort to relax state and federal restrictions on the sharing of customer information, particularly information involving non-published telephone numbers. Other issues that need to be addressed are existing constraints on non-payment disconnections and prohibitions against the denial of new residential service to persons with a history of fraudulent use.

C. ACTION TO ENCOURAGE COOPERATION AMONG SERVICE PROVIDERS.

The Commission also could require all entities subject to its jurisdiction to work cooperatively to fight toll fraud.[46] Existing toll fraud detection and prevention efforts are not always coordinated, nor is there always full and timely cooperation between all involved equipment and service providers. Thus, the Commission could create an agency, similar to the National Exchange Carriers Association, with a charter to serve

---

[46] This would include not only common carriers, but also equipment manufacturers that are subject to Part 68.

agency, similar to the National Exchange Carriers Association, with a charter to serve as a centralized toll fraud prevention and detection agency. The purpose of that agency should include serving as a centralized:

- Repository of data related to toll fraud, the perpetrators, and their method(s) of operation, including establishing a suspicious number list for the use of LIDB owners;
- Clearing house for the dissemination of information regarding ongoing fraud schemes;
- Clearing house for data related to deterrence equipment and methods; and
- Education and training bureau.

It is also important for the Commission to clarify that the creation of an agency to coordinate toll fraud prevention would not imply that the agency is somehow assuming responsibility for fraud prevention or liability for losses. There are other entities that also could make useful contributions on a voluntary basis such as associations representing payphone providers. The Commission should encourage those entities to participate as well.

D. ENFORCEMENT LEGISLATION.

The Commission requests comment on whether it should encourage Congressional legislation that would clearly define and penalize toll fraud, and give law enforcement agencies the tools needed to track and prosecute perpetrators of toll fraud. (*NPRM* at ¶ 13.) GTE wholeheartedly endorses any assistance the Commission could offer to accomplish these important tasks.

GTE's telephone operating companies have experienced many frustrations in prosecuting toll fraud perpetrators. In many cases, law enforcement agencies are hampered by cumbersome laws that prevent the rapid action that is necessary to obtain the evidence that would provide a reasonable chance of securing a conviction. Toll

fraud perpetrators typically act within a very narrow window of opportunity, often only a matter of days. Many laws governing the process of obtaining subpoenas, search warrants and/or court orders do not permit the swift action necessary to deal with this dynamic form of criminal activity. If law enforcement agencies cannot respond quickly, the opportunity to apprehend or successfully prosecute criminals may be lost forever. Congressional action to address these shortcomings in existing laws is critical to efforts to deter toll fraud through successful prosecution of criminals.

In summary: It is not necessary for the Commission to attempt to reinforce the incentives for toll fraud prevention and detection that already exist. Rather, the Commission can assist the telecommunications industry by: (i) encouraging organizations representing the interests of private payphone providers to educate their members on fraud prevention techniques; (ii) leading an effort to relax state and federal restrictions on the sharing of customer information needed to identify and combat toll fraud; (iii) require all entities subject to its jurisdiction to cooperate with a new agency that should be created to coordinate detection and prevention efforts; and (iv) encouraging a Congressional effort to create legislation that would clearly define and penalize toll fraud and give law enforcement agencies the tools needed to track and prosecute perpetrators of toll fraud.

Respectfully submitted,

GTE Service Corporation and its affiliated domestic telephone, equipment and service companies

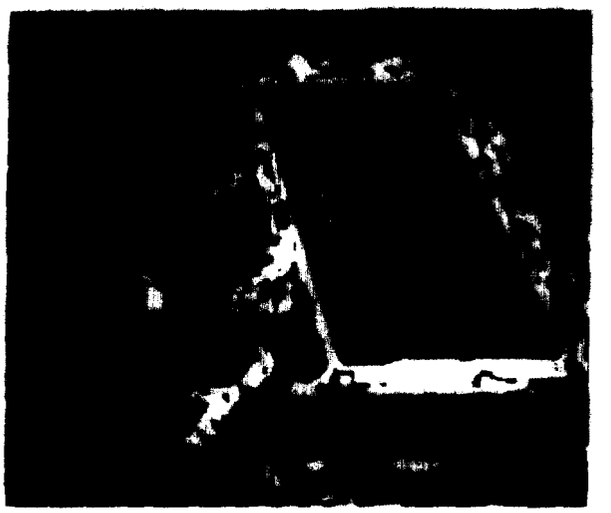
David J. Gudino
1850 M Street, N.W.
Suite 1200
Washington, DC 20036
(202) 463-5212

January 14, 1994

Their Attorney

ATTACHMENT A

Tips to Help Deter Toll Fraud



GTEL GTE

©1992 GTE Telephone Operations
Control No. 6012A 10/92

GTEL is concerned about toll fraud.While it is impossible to completely protect telecommunication systems against toll fraud, the following tips from GTEL can help reduce the risk.

- Use telephone credit cards rather than the DISA feature in the Private Automatic Branch Exchange (PBX).
- If DISA is utilized in your system, change the passwords frequently; implement a program to monitor call detail records on a daily basis and make the passwords at least six digits in length.
- Deactivate unused phone extensions as soon as they are no longer needed.
- Restrict area codes in the PBX for countries that are never called.
- Use time-of-day restrictions to control after-hours dialing.
- Have authorization codes assigned to stations to allow you to track who made the call, no matter where the call originated.
- Restrict the circulation of PBX system information (i.e., passwords, authorization codes, etc.).
- Limit the call-forwarding external feature to those who really need it.
- Avoid transferring calls from callers outside the system without proper identification and verification. This abuse most often takes place when a system operator receives an external call from someone identifying themselves as an employee and requesting the operator to connect them to a long-distance number.
- Monitor the call detail reports daily for unusual changes in usage patterns.
- Use a paper shredder to destroy any PBX system information that would be useful to hackers.
- Use multiple levels of passwords to access the system data base. Periodically change these passwords. Never allow the use of default passwords on any equipment.
- Have employees sign non-disclosure agreements pertaining to PBX passwords.
- If you have INWATS (i.e., 800 service) and ISDN Primary Rate Interface (PRI), utilize the automatic number identification provided by ISDN PRI to block out unauthorized calls coming in on the 800 numbers.
- If you have voicemail, program your voicemail system so that it will not transfer a caller to an outside line.
- Put a verbal warning on the voicemail system stating those utilizing the system illegally will be prosecuted.

GTEL assumes no responsibility for losses due to toll fraud; however, your GTEL Account Executive or GTEL Telephone Account Manager will be happy to assist you in taking preventive measures.

PBX HACKING and TOLL FRAUD

TOLL FRAUD EXCEEDS $500 MILLION PER YEAR !!!

You may be in good company!

MITSUBISHI $430,000

PERKINS ELMER $250,000

PACIFIC MUTUAL $200,000

ICF INTERNATIONAL $82,000

UNITED NATIONS $1,000,000

ITT $100,000

NYC HUMAN RESOURCE ADMINISTRATION $528,000

PROCTOR & GAMBLE $300,000

NASA $12,000,000

DRUG ENFORCEMENT AGENCY $2,000,000

WHO IS MOST "AT RISK"?

1-800 In-Wats type service terminating on DISA (Direct Inward System Access) or Automated Attendant and Voice Mail Systems.

PBX HACKING and TOLL FRAUD

- PRANKING

Voice Mail Box

System Administrator Port

- PIRACY

Fraudulent Long Distance Calls

- DISA

- Auto Attendant / Voice Mail Call Processing

HACKING

Common Voice Mail **"pranking".**

Access Code or Password hacking for personal fraudulent use or for resale and fraudulent use of your phone service.

System Administration hacking of your PBX and Voicemail Systems.

Who Does It?

Hackers / "Phreakers"

Call - Sell Operators

Drug Dealers and Bookies

Industrial Spies

How it's done.

Auto Dial Modem

Dial every 800 NNX-XXXX or every NNX-XXXX of a **target** range of numbers.

Target XYZ Company by looking up main listed number in directory to determine NNX-XXXX range being used.

or

Obtain a directory of 800 numbers and pick a victim.

or

Information and numbers from an electronic bulletin board.

Modem software program will list every number dialed that received a modem tone or DISA prompt.

Hacker may then attempt to hack desired Voice Mail box, modem, or DISA entry.

The Auto Dial Modem may be programmed to dial thousands of combinations of digits overnight and list those that work.

How hard is it?

Number of Digits In the Password	Odds of Correctly Finding the Password
1	1 in 9
2	1 in 90
3	1 in 900
4	1 in 9,000
5	1 in 90,000
6	1 in 900,000
7	1 in 9,000,000
8	1 in 90,000,000
9	1 in 900,000,000
10	1 in 9,000,000,000
11	1 in 90,000,000,000
12	1 in 900,000,000,000
13	1 in 9,000,000,000,000
14	1 in 90,000,000,000,000
15	1 in 900,000,000,000,000

NOTE: 4 digits can be broken in under 1 hour!!

VOICE MAIL HACKING

What do they do?

Break user password and "prank". Verbal graffiti.

Break user password and take over the mail box by changing the password and greeting.

Break default password on unassigned mail boxes and change the password and greeting.

Break user password and listen to or record confidential information. Industrial Spies!

What do they use the Mail Box for?

Personal use.

Pass Hacking information to other hackers.

Conduct other illegal activities;
ie: Drug Deals, Stolen Credit Card Numbers, Bookies, etc.

Sell these compromised mail boxes to others.

Industrial Espionage;
- Confidential Messages listened to, recorded, deleted.
- Bring Voice Mail System Down
- Leave bogus messages

What can be done?

The responsibility to maintain the security and integrity of the Voice Mail System belongs to the end user company System Administrator and the individual users on the system.

THREE LEVELS OF SECURITY

Company Security

System Security

User Security

System Administrator Responsibilities

- Detection

Monitor System Reports for;

Excessive after hours use.

Password access and unsuccessful attempts.

Check all defined mail boxes to ensure they belong to current employees only. Delete all others.

Unusual out-dialing patterns.

Reduction in storage capacity.

Investigate user complaints of;

Messages not received.

Enrolled users locked-out of system; ie, password changed.

Obscene messages or altered greetings.

- Security Procedures to Implement

Do not build spare mailboxes ahead of time.

Do not leave default passwords on any mail box.

Remove immediately mail boxes when someone leaves.

Require individual users to set long and random passwords.

Require users to change passwords periodically.

Program invalid password attempts to;

1. Disconnect caller.
2. Transfer to attendant (in order to detect hacking attempts and keep a log).

Reconsider the use of allowing Name Dialing access to mail boxes. Why provide easy directory access for Industrial Spies.

Install ANI (Automated Number Identification), if available on your system.

Do not assign predictable System Administration port extension numbers; ie, x500, x199. Make it difficult to find the Administration port to hack.

- **What to look for in a Voice Mail System**

Easy to change user passwords (so they will do it).

Flexible Password length (make them different lengths).

Reports that are useful in detecting hacking.

Built in limits on the number of invalid password attempts before disconnect or transfer out of system. (Beware of how you handle the transfer - don't set yourself up for toll fraud.)

Automatic system prompting of users to change their password.

Ability of System Administrator to change user passwords.

Multiple levels of Administrative access and passwords.

SYSTEM ADMINISTRATION PORT HACKING

Voice Mail Administration Port

PBX System Administration Port

Your system is vulnerable to "pranking," Industrial Espionage, and Toll Fraud through these ports!!!

Consider the use of Dial Back Modems.

Don't use predictable extension numbers for these ports; ie, x500, x199

Set System Administration password to the maximum number of digits,

and set multiple levels of access if available or appropriate on your system.

Notify local service provider of any changes in System Administration passwords if remote maintenance is required.

Write down password and keep in a secure place.

When creating temporary user passwords, use unique random number. Do not use the system default.

Do not provide direct modem access to Administration ports.

TOLL FRAUD

**** PIRACY!! ****

Your PBX **will be** hacked so that calls can be placed as if they were originated from inside your system. Entry most likely will be through 1-800 trunks terminating on your system.

TOLL FRAUD ACCESS

Attendant

Auto Attendant and Voice Mail (Thru - Dial)

DISA

AT&T Call Manager (ACM)

TOLL FRAUD

Who does it?

Amateur Hackers

Same people that hack Voice Mail Systems.

Usually smaller dollar amount of fraud.

Personal or limited use.

Dialing information is passed to other hackers over electronic bulletin boards or over "hacked" voice mail boxes.

Abuse can be undetected for months.

Often codes are sold to the **Professionals**.

Insiders

Disgruntled employees.

Ex-employees

Technicians or others in the industry with knowledge about access.

Like the Amateurs, the damage is usually limited unless the information is obtained by **Professionals.**

Professionals

Typically operate out of New York (area code 212 or 218)

Fraudulent calls are all to "third world" countries.

Tremendous volume of calls over a short period of time;
ie, several thousand calls over a weekend representing $60,000 to

$100,000 worth of fraud, limited only by the size of your facilities.

Very well organized call-sell operations marketing to recent immigrant communities. Typically, 100% of the fraudulent calls are to one country.

Other customers include Institutions like colleges, prisons, and military installations.

Access into to your switch is through your 1-800 trunks.

How do they obtain Access Information?

They are themselves or they employ very technologically sophisticated and industry knowledgeable individuals.

Purchase the information from Amateur Hackers.

Theft

Data Base Penetration

Internal Sources

Attendant Access Fraud

Switchboard Operator

"Dupe your switchboard operator"

Access your attendant (switchboard operator) via 1-800 trunk or DID and ask for any valid extension or individual.

Upon answer, claim wrong # and ask to be transferred back to the attendant.

Returned call appears as an internal call to the attendant.